Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version 1.5

Victorian Protective Data Security Standards

Version 1.5

Document details

Version	Publish date	Amendments in this version
1.0	June 2016	n/a
1.1	March 2018	• Updated some control references

2.0	September 2019	• Removed protocols
		• Integrated elements including a mapping to their control reference derivation and the old and new numbering
		• Updated reference sources where the elements have been derived from
		• Globally replace ‘protective data security’ with ‘information security’
		• Globally replace ‘public sector data’ with ‘official information’
		• Merged the following standards
		  ○ 1, 3
		  ○ 2, 11
		  ○ 5, 6
		  ○ 9, 10, 15
		  ○ 13, 14
		• Replace Standard 12 – Compliance with new standard on reporting
		• Globally change language to active voice

Victorian Protective Data Security Standards

Version 1.5

The purpose of the Victorian Protective Data Security Standards (VPDSS) is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information. The Standards are issued under Parts 4 and 5 of the Privacy and Data Protection Act 2014.

Objectives

The VPDSS is developed to help Victorian public sector organisations:

- manage information throughout its lifecycle (creation to disposal)
- manage information across all the security domains (information, personnel, Information Communications Technology (ICT), physical)
- manage security risks to the confidentiality, integrity and availability (CIA) of official information
- manage external parties with access to information
- share information with other agencies with confidence
- minimise security incidents.

Security Domains

There are 12 Victorian Protective Data Standards (Standards). Standards 1 to 8 relate to overarching information governance or topics that cover multiple security domains. The remaining standards relate to different areas or 'domains' of information security. Standard 9 relates to information security aspects of information management, Standard 10 relates to personnel security, Standard 11 relates to ICT security and Standard 12 relates to physical security.

Structure of the VPDSS

VPDSS Structure	Description	Outcome
Title	Heading/name of the standard	Key topic area (informational)
Standard	High-level statement describing what needs to be achieved by the organisation.	What is required (mandatory)
Statement of	A statement of the intent of the standard identifying the	Why it is required

Objective	desired outcome when the standard has been achieved.	(informational)
Element	A security measure(s) extracted from the source reference point that provide high level guidance on baseline or minimum controls.	How to? (risk-based action)
Derivation	Source reference point where the element has been derived from for further implementation advice. References include Australian and International Standards, Federal and State government guidance and tailored guides developed by OVIC.	Need more information? (informational)

A word on elements

Elements are a security measure that modifies risk. Elements often depend on a supportive control environment to be effective. A control environment can be a set of standards, processes and structures that provide the basis for applying controls across the organisation. The control environment therefore contributes to modifying risk indirectly.

The elements described in the VPDSS include both controls that directly modify risk and supportive controls that are essential to the control environment. Organisations should determine and implement specific controls (which may be the element itself or multiple controls that fall under the element) appropriate to their organisation considering their internal and external context and risks.

The determination of applicable elements depends upon the organisation's criteria for risk acceptance and risk treatment options. Element determination also depends on the manners in which elements interact with one another to provide 'defence in depth'[*]. Whilst the elements have been logically grouped under their related topic area i.e. elements related to physical security are listed under the physical security Standard, selection of elements to mitigate risks may not be isolated to the specific topic area.

OVIC has provided the derivation or source documents with specific reference to the sections where each element has been derived for further information regarding implementation of them. Organisations can design their own controls as required or identify them from any source that have at least functional equiveillance or better as the element identified by OVIC. Where elements are deemed not applicable to an organisation, supporting justification should accompany such decisions.

[*] Defence in depth is a multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access. This approach works on the premise that where one measure fails, there is another independent method in place to continue to defend.

Standard 1 – Information Security Management Framework

Standard

An organisation establishes, implements and maintains an information security management framework relevant to its size, resources and risk posture.

Statement of Objective

To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E1.010	SMF-010	The organisation documents an information security management framework covering governance arrangements and the security domains of information, personnel, ICT and physical.	*AS ISO/IEC 27001:2015* § 4 § 5.2
E1.020	SMF-020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	*AS ISO/IEC 27001:2015* § 4.2
E1.030	COM-020	The organisation identifies information security performance indicators and monitors information security obligations against these.	*AS ISO/IEC 27001:2015* § 9
E1.040	SMF-030	Executive management endorses and sponsors information security.	*AS ISO/IEC 27001:2015* § 5.1
E1.050	SMF-040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.	*AS ISO/IEC 27001:2015* § 5.3
E1.060	SMF-050	The organisation refers to its risk management framework in the information security management framework.	*AS ISO/IEC 27001:2015* § 6.1
E1.070	SMF-070	Executive management commits to providing sufficient resources to support information security.	*AS ISO/IEC 27001:2015* § 7.1 § 7.2
E1.080	SMF-080	The organisation sufficiently communicates its information security management framework and	*AS ISO/IEC 27001:2015*

		ensures it is accessible.	§ 7.4
E1.090	SMF-060	Executive management establishes and communicates an information security strategy and implementation plan.	*AS ISO/IEC 27001:2015* § 6.2
E1.100		The organisation documents its control framework/library that addresses its information security risks.	*AS ISO/IEC 27001:2015* § 6.1
E1.110	SMF-090	The organisation monitors, reviews, validates and updates the information security management framework.	*AS ISO/IEC 27001:2015* § 9

Change log

Title
- Add 'information'

Standard
- Add 'information'
- Replace 'proportionate' with 'relevant'
- Change to active voice (removes 'must' language)

Objective
- Replace 'public sector data' with 'official information'
- Change to active voice

Control references/derivation
- No change

Elements
- Replace 'protective data security' with 'information security'
- Incorporate SPP-010 into SMF-010
- Re-order SMF-060 for logical sequencing
- Remove SPP-020 (covered generically by SMF-010)
- Remove SPP-030 (covered under SMF-030)
- Remove SPP-040 (covered under SMF-090)
- Add new element E1.100 to refer to control framework/library in use by the organisation which may be a combination of various sources ISO, PSPF, NIST, COBIT etc depending on their environment
- Move COM-020 from V1.1 Standard 12 Compliance for better fit to SMF activities and re-order to define indicators before measuring against these
- Change to active voice

Standard 2 – Information Security Risk Management

Standard

An organisation utilises a risk management framework to manage information security risks.

Statement of Objective

To ensure that an organisation manages information security risks through informed business decisions while applying controls to protect official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E2.010	SRM-010	The organisation manages information security risks in accordance with its risk management framework.	*AS ISO/IEC 27005:2015* § 5 *AS ISO/IEC 27005:2015* § 7.3 *AS ISO 31000:2018* § 5.3
E2.020	SRM-020	The organisation conducts security risk profile assessments to identify, analyse and evaluate options to manage information security risks.	*VPDSF Assurance Collection* § Chapter 1 PDSRPA *AS ISO/IEC 27001:2015* § 6.1
E2.030	RTP-020	The executive management documents and approves its protective data security plan (PDSP).	*VPDSF Assurance Collection Chapter 3* § 17
E2.040	SRM-030	The organisation records information security risks in its risk register.	*VMIA Practice Guide* Risk Process - Risk Register *AS ISO 31000:2018* § 6.7
E2.050	SRM-040	The organisation includes Information security risks in organisational planning.	*VGRMF* § Appendix 1 Risk management concepts *VMIA Practice Guide* § Risk Governance - Corporate and Business

			Planning
E2.060	SRM-050	The organisation collaborates with internal and external stakeholders during the information security risk management process.	*VPDSF Assurance Collection Chapter 1* § PDSRPA – Consultation *VMIA Practice Guide* § Risk Process *AS ISO/IEC 27005:2015* § 7.4 *AS ISO/IEC 27005:2015* § 11 *AS ISO 31000:2018* § 6.2
E2.070	SRM-060	The organisation regularly reviews its threat environment.	*VPDSF Assurance Collection Chapter 1* § 11 *VMIA Practice Guide* § Risk Management - Risk Profile Review § Risk Process *AS ISO/IEC 27005:2015* § 12.2 *AS ISO 31000:2018* § 6.6
E2.080	SRM-070	The organisation governs, monitors, reviews and reports on information security risk through an audit committee (or equivalent).	*VGRMF* § 2.2.2 *AS ISO 31000:2018* § 5.2 *AS ISO 31000:2018* § 6.7

Change log

Title

- Add ‘information’

Standard

- Add ‘information’
- Change to active voice (removes ‘must’ language)

Objective

- Utilise objective from ‘Standard 11 Security Plans’
- Replace ‘treats identified’ with more generic and encompassing term ‘manages’
- Remove ‘cost-effective security’ to be more generic that the controls may or may not be specific to security
- Replace ‘public sector data’ with ‘official information’

Control references/derivation

- Add reference to AS ISO/IEC 27005:2015 Information Security Risk Management
- Add reference to VMIA Risk Practice Guide

Elements

- SRM-010 Reword to clarify that security risks should be dealt the same way as other business risks and you don’t have to create a new risk process to manage them
- SRM-020 Replace ‘security risks to information assets’ with ‘information security risks’
- SRM-020 Add ‘analyse and evaluate options to manage’ to cover the risk assessment process
- SRM-030, SRM-040, SRM-050, SRM-070 Add ‘information’
- SRM-030 Remove ‘identified’ because doesn’t add value
- SRM-060 Replace ‘security risk profile’ with threat environment to use more commonly understood language
- Remove RTP-010 (covered under SRM-040)
- Move RTP-020 to come after SRPA
- Modify RTP-020 to reside with executive management
- Remove RTP-030 (covered under RTP-020)
- Change to active voice

Standard 3 – Information Access

Standard

An organisation establishes, implements and maintains an access management process for controlling access to official information.

Statement of Objective

To formally authorise and manage the physical and logical access to official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E3.010	IAM-010	The organisation has an identity and access management policy covering physical and logical access to official information.	*AS ISO/IEC 27002:2015* § 9.1.1 *SOD IDAM 01 – Workforce Identity and Access Management*[†] § IdAM Governance
E3.020	IAM-020	The organisation has a process for managing identities and the issuance of secure credentials (registration and de-registration) for physical and logical access to official information.	*AS ISO/IEC 27002:2015* § 9.2 *SOD IDAM 01 – Workforce Identity and Access Management* § Enrolment
E3.030	IAM-030	The organisation track access to and use of, important official information e.g. classified document register.	No parent reference
E3.040	IAM-040	The organisation has physical access controls.	*AS ISO/IEC 27002:2015* § 11.1.1 § 11.1.2
E3.050	IAM-050	The organisation has logical access controls.	*AS ISO/IEC 27002:2015* § 9.1.2

[†] The Victorian Government Workforce IdAM Statement of Direction defines the whole of government vision for identity and access management. Whilst a government wide approach, the areas covered in this document can also be applied at a local organisation level.

			§ 9.2.1 § 9.4 *Australian Government Information Security Manual (ISM)* § Guidelines for system hardening – System access
E3.060	IAM-070	The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.	*AS ISO/IEC 27002:2015* § 9.2.2 *SOD IDAM 01 – Workforce Identity and Access Management* § Lifecycle Management
E3.070	IAM-080	The organisation limits the use of, and actively manages privileged physical and logical access e.g. administrator accounts, and separates these from normal access accounts.	*AS ISO/IEC 27002:2015* § 9.2.3 *SOD IDAM 01 – Workforce Identity and Access Management*[‡] § Privileged Access
E3.080		The organisation regularly reviews and adjusts access rights.	*AS ISO/IEC 27002:2015* § 9.2.5 § 9.2.6

Change log

Title

- Change number from Standard 4 to Standard 3

Standard

- Replace ‘regime’ with ‘process’
- Replace ‘public sector data’ with ‘official information’
- Add ‘controlling’ access rather than ‘for access’
- Change to active voice (removes ‘must’ language)

Objective

[‡] The Victorian Government Workforce IdAM Statement of Direction defines the whole of government vision for identity and access management. Whilst a government approach, the areas covered in this document can also be applied at a local organisation level.

- Replace ‘public sector data’ with ‘official information’
- Explicitly state physical and logical methods of access
- Replace ‘controlled across the core security domains’ with ‘managed’
- Change to active voice

Control references/Derivation

- Remove reference to NIST

Elements

- Modify IAM-030 to replace ‘key’ with ‘important’
- Remove duplicate IAM-060 and better integrate into IAM-020
- Elaborate IAM-080 to provide an example of a privileged account and add ‘limit the use of’
- Add new element E3.080 regarding review of access rights
- Change to active voice

Standard 4 – Information Security Culture

Standard

An organisation ensures all persons with access to official information understand their security obligations.

Statement of Objective

Creating and maintaining a strong security culture by ensuring that all persons understand the importance of information security across the security domains and their obligations for protecting official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E4.010	SOP-010	The organisation documents information security obligations of all persons.	*PSPF GOVSEC-2 Management structures and responsibilities* § C.8 *AS ISO/IEC 27002:2015* § 7.2.1
E4.020	STA-030	The organisation's information security training and awareness content covers all security domains.	*PSPF GOVSEC-2 Management structures and responsibilities* § C.9 para 61 § C.9.2
E4.030	STA-020	The organisation delivers information security training and awareness to all persons, upon engagement and regular intervals thereafter in accordance with its training and awareness program and schedule.	*PSPF GOVSEC-2 Management structures and responsibilities* § C.9 § C.9.3 *AS ISO/IEC 27002:2015* § 7.2.2
E4.040	STA-040	The organisation provides targeted information security training and awareness to persons in high risk functions or who have specific security obligations.	*PSPF GOVSEC-2 Management structures and responsibilities* § C.9 para 61

			§ C.9.2
E4.050	SOP-020	The organisation seeks reaffirmation of all person's information security obligations at defined intervals.	*PSPF GOVSEC-2 Management structures and responsibilities* § C.9.3
E4.060	STA-060	The organisation monitors, reviews, validates and updates its information security training and awareness program and schedule.	*AS ISO/IEC 27002:2015* § 7.2.2

Change log

Title

- Change numbering from Standard 6 and 7 to Standard 3
- Due to the merging of two standards, change 'Security Obligations' and Security Training and Awareness' to an overarching term 'Information Security Culture'

Standard

- Replace 'public sector data' with 'official information'
- Replace Security Training and Awareness' standard wording from 'security training and awareness' to 'their security obligations'
- Change to active voice (removes 'must' language)

Objective

- Replace 'public sector data' with 'official information'
- Change to active voice
- Remove 'core' and retain as general security domains

Control references/Derivation

- Replace PSPF references with updated version

Elements

- Add 'information' to 'security training and awareness'
- Reorder for logical sequencing
- Remove STA-010 Inferred by SMF-080 and STA-020
- Merge STA-020 and STA-050 to incorporate establishing as well as delivering a program and be more specific of what the requirement is i.e. program (delivery mechanisms) and supported by a schedule
- Add 'the organisation's' to make statements more complete and accountability clear
- STA-040 Replace 'roles' with 'functions' to cover specific duties that may be part of positions
- SOP-020 Reorder wording to make 'organisation' driven activity
- SOP-030 Remove (covered in STA-060)
- STA-060 Add 'and schedule' to be consistent with STA-050
- Change to active voice

Standard 5 – Information Security Incident Management

Standard

An organisation establishes, implements and maintains an information security incident management process relevant to its size, resources and risk posture.

Statement of Objective

To ensure a consistent approach for managing information security incidents, in order to minimise organisational impact.

Elements

V2.0 #	V1.1 #	Element	Derivation
E5.010	SIM-010	The organisation has information security incident management policies and procedures covering all security domains.	*AS ISO/IEC 27002:2015* § 16.1.1 *PSPF GOVSEC-2* § C.7
E5.020	SIM-020	The organisation articulates roles and responsibilities for information security incident management.	*AS ISO/IEC 27002:2015* § 16.1.1
E5.030	SIM-040	The organisation's information security incident management policies and procedures contain the five phases of: * Plan and prepare * Detect and report * Assess and decide * Respond * Lessons learnt	*VPDSF Security Incident Management Framework* § A Preparation *WoVG Cyber Incident Management Plan* § Managing Cyber Incidents *AS ISO/IEC 27002:2015* § 16.1.1 *AS ISO/IEC 27035.1:2017* § 5 *PSPF GOVSEC-2* § Annex A

E5.040	SIM-050	The organisation records information security incidents in a register.	*PSPF GOVSEC-2* § C.7 § Annex A Step 1 *AS ISO/IEC 27035.2:2017* § Annex B.2.2
E5.050	SIM-060	The organisation's information security incident management procedures identify and categorise administrative vs criminal incidents and investigative handover.	*PSPF GOVSEC-2* § C.7 § Annex B
E5.060		The organisation regularly tests its incident response plan.	*WoVG Cyber Incident Management Plan* § Managing Cyber Incidents

Change Log

Title
- Change numbering from Standard 7 to Standard 5
- Add 'information'

Standard
- Add 'information'
- Replace 'regime' with 'process'
- Replace 'proportionate' with 'relevant'
- Change to active voice (removes 'must' language)

Objective
- Add 'information'
- Replace 'allowing timely corrective action to be taken for the protection of public sector data' to 'in order to minimise organisational impact'
- Change to active voice e.g. 'managing,' 'protecting'

Control references / Derivation
- Replace PSPF reference with GOVSEC-2 Management structures and responsibilities
- Add AS ISO/IEC 27002:2015 Code of practice for information security controls
- Add AS ISO/IEC 27035.1:2017 Principles of incident management
- Add AS ISO/IEC 27035.2:2017 Guidelines to plan and prepare for incident response

Elements
- SIM-010, SIM-020, SIM-040, SIM-050, SIM-060 Add 'information'
- SIM-010 Remove 'protective data'
- SIM-020 Replace 'accountabilities' with 'responsibilities'
- Remove SIM-030 (covered under SIM-040)
- Remove SIM-070 (covered under SIM-040)
- Add new element E5.060 to test the plan
- Change to active voice

Standard 6 – Information Security Aspects of Business Continuity

Standard

An organisation embeds information security continuity in its business continuity management program.

Statement of Objective

To enhance an organisation's capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E6.010	BCM-010	The organisation includes all facets of information security in its business continuity management policies and plans.	*AS ISO/IEC 27002:2015* § 17.1.1
E6.020	ICT-030	The organisation includes information security requirements in disaster recovery plans for ICT systems.	*AS ISO/IEC 27002:2015* § 17.1
E6.030	BCM-020	The organisation identifies and assigns roles and responsibilities for information security in business continuity management policies and plans.	*AS ISO/IEC 27002:2015* § 17.1.2
E6.040	BCM-040	The organisation monitors, reviews, validates and updates the information security requirements of its business continuity management policies and plans.	*AS ISO/IEC 27002:2015* § 17.1.3

Change log

Title

- Change numbering from Standard 8 to Standard 6
- Replace 'Business Continuity Management' with 'Information Security Aspects of Business Continuity'

Standard

- Reword to be clear that this standard is referring to considering information security in an adverse situation rather than developing a business continuity framework which is a separate discipline that should already be in place. Replace '*establish, implement and maintain a business continuity management program that addresses the security of public sector data'* with '*embed information security continuity in its business continuity management program'*
- Change to active voice (removes 'must' language)

Objective

- Replace 'public sector data' with 'official information'

Control references / Derivation

- Move away from referencing business continuity specific guidance such as AS5050 and ISO22301 as this should already be in place
- ANAO Business Continuity Management better practice guide withdrawn

- Add reference to AS ISO/IEC 27002:2015 Code of practice for information security controls

Elements

- Replace BCM-010 with clearer language regarding the requirement to think of how information is protected in an adverse situation
- BCM-010, BCM-020, BCM-040 Replace ‘protective data’ with ‘information’
- Remove BCM-030 as the communications plan is generically covered under BCM-010 policies and plans
- Refer to ‘business continuity management policies and plans’ throughout all elements for consistency
- Move ICT-030 related to disaster recovery plans from Standard 11 – ICT Security
- ICT-030 Add ‘include information security requirements’ of disaster recovery to distinguish from normal operational IT availability requirements
- Change to active voice

Standard 7 – Third Party Arrangements

Standard

An organisation ensures that third parties securely collect, hold, manage, use, disclose or transfer official information.

Statement of Objective

To confirm that the organisation's official information is protected when they interact and/or engage with a third party.

Elements

V2.0 #	V1.1 #	Element	Derivation
E7.010	SUP-010	The organisation's information security policies, procedures and controls cover the entire lifecycle of third party arrangements (including contracts, MOUs and information sharing agreements).	*AS ISO/IEC 27002:2015* § 13.2.1 § 15.1.1
E7.020	SUP-020	The organisation includes requirements from all security domains in third party arrangements (including contracts, MOUs and information sharing agreements).	*PSPF GOVSEC-6* § C.2 *AS ISO/IEC 27002:2015* § 13.2.2 § 13.2.4 § 15.1.2
E7.030	SUP-030	The organisation risk assesses any security controls to be included in third party arrangements, in the third party's environment before finalising arrangements.	*PSPF GOVSEC-6* § C.3.1 (para 21.c)
E7.040	SUP-040	The organisation applies appropriate security controls upon cessation of a third party arrangement (including contracts, MOUs and information sharing agreements).	*PSPF GOVSEC-6* § C.4
E7.050	SUP-050	The organisation identifies and assigns information security roles and responsibilities in third party arrangements (including contracts, MOUs and information sharing agreements).	*AS ISO/IEC 27002:2015* § 15.2.1
E7.060	INS-040	The organisation establishes, maintains and reviews a register of third party arrangements (including contracts, MOUs and information sharing	*No parent reference*

		agreements).	
E7.070	SUP-070	The organisation monitors, reviews, validates and updates the information security requirements of third party arrangements and activities.	*PSPF GOVSEC-6* § C.3 *AS ISO/IEC 27002:2015* § 15.2.1 *PDP Act* § 89 (3)
E7.080		The organisation documents its information release management requirements including the obligations of all parties and the lifecycle of any official information that is formally released.	*No parent reference*

Change log

Title

- Change numbering from Standard 9, 10 and 15 to Standard 7
- Due to the merging of three standards, change 'Contracted Service Providers', 'Government Services' and 'Information Sharing' to an overarching term 'Third Party Arrangements'

Standard

- Replace 'contracted service providers' with 'third parties'
- Replace 'public sector data' with 'official information'
- Simplify to remove legalese wording 'do not do an act…' and replace with information handling stages
- Change to active voice (removes 'must' language)

Objective

- Replace 'public sector data' with 'official information'
- Replace 'contracted service provider' with 'third party'
- Replace with wording from Standard 10

Controls

- PSPF reference no longer exists
- ANAO reference no longer exists
- Add reference to 27002 and PSPF GOVSEC 6

Elements

- Remove 'protective data'
- Replace 'supplier' with 'third party'
- Replace 'service' with 'third party'
- SUP-010 Add 'information security policies'
- SUP-010 Replace 'management' to 'arrangements'
- Modify SUP-030 to be clear this should be risk assessed
- Modify SUP-040 to be more generic regarding returning to normal operations post third party arrangements to apply relevant remediation controls as agreed by both parties
- SUP-050 Replace 'protective data' with 'information'
- Incorporate SUP-060 into SUP-010 and remove SUP-060

- SUP-070 Add ‘information’ to be more specific
- SUP-070 Add ‘activities’ so it includes all areas of the engagement not just the contract/agreement
- Remove INS-010 (covered under SUP-010)
- Remove INS-020 (covered under SUP-020)
- Remove INS-030 (covered under SUP-030)
- Modify INS-040 to include a register of all third party arrangements not just information sharing arrangements
- Remove INS-050 (covered under SUP-070)
- Add new element E7.080 regarding ‘information release’
- Change to active voice

Standard 8 – Information Security Reporting to OVIC

Standard

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner.

Statement of Objective

To promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks.

Elements

V2.0 #	V1.1 #	Element	Derivation
E8.010		The organisation notifies OVIC of incidents that have a business impact level (BIL) on the confidentiality, integrity or availability of official information of 2 (limited) or higher[§].	No mapping
E8.020		The organisation submits its completed Protective Data Security Plan (PDSP) to OVIC every two years.	*PDP Act* § 89 4 (b)
E8.030		Upon significant change, the organisation submits its reviewed Protective Data Security Plan (PDSP) to OVIC.	*PDP Act* § 89 4 (a)
E8.040		The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	*VPDSF Assurance Collection Chapter 4?*

Change log

Title

- Change numbering from Standard 12 to Standard 8
- Change from 'Compliance' to 'Information Security Reporting' to be explicit regarding the reporting requirements of agencies to OVIC

Standard

- Move from annual assessment of compliance and reporting with the VPDSS to cover regular reporting of all VPDSS requirements to OVIC
- Change to active voice (removes 'must' language)

Objective

- Replace 'compliance' with 'implementation'
- Replace 'VPDSS' with 'information security'

Controls

- Remove reference to AS/ ISO 19600 Compliance Management System

Elements

- COM-010 Remove because captured under generic security risk analysis SRM-020

[§] Refer to the current VPDSF BIL table on the OVIC website https://ovic.vic.gov.au/resource/vpdsf-business-impact-level-table-v2-0/ for further information.

- COM-010 Move to Standard 2 – Information Security Risk Management
- COM-020 Move to Standard 1 – Information Security Management Framework
- COM-030 Split into new elements E8.010-8.040 which each cover the respective reporting requirements including incident notification as it occurs, biennial and significant change PDSP submission and annual attestation
- COM-040 Remove independent audit requirements because it doesn't account for all types and sizes of organisations

Standard 9 – Security Aspects of Information Management

Standard

An organisation identifies and assesses the value of official information.

Statement of Objective

To ensure an organisation uses consistent identification and assessment criteria for official information across its lifecycle to maintain its confidentiality, integrity and availability.

Elements

V2.0 #	V1.1 #	Element	Derivation
E9.010	INM-010	The organisation's Information Management Framework incorporates all information security domains.	*WoVG Information Management Framework* § Enabler: Security and Privacy § Enabler: Lifecycle Management
E9.020	INF-010	The organisation defines its information asset types.	*VPDSF Information Security Management Collection Chapter 1 – Identifying and Managing Information Assets* § 9
E9.030	INF-020	The organisation conducts an information review to identify its information assets in consultation with its internal stakeholders.	*VPDSF Information Security Management Collection Chapter 1 – Identifying and Managing Information Assets* § 8
E9.040	INF-040	The organisation establishes and manages an information asset register.	*VPDSF Information Security Management Collection Chapter 1 – Identifying and Managing Information Assets*

			§ 10
E9.050	INF-050	The organisation identifies roles and responsibilities for assets in its information asset register e.g. originator, owner, custodian.	*VPDSF Information Security Management Collection* § Chapter 1 – Appendix D
E9.060	INF-060	The organisation uses the VPDSF business impact level table to value official information.	*VPDSF Information Security Management Collection Chapter 2 – Understanding Information Value* § 17
E9.070	INF-030	The organisation identifies and documents the security attributes (confidentiality, integrity and availability business impact levels) of its information assets.	*VPDSF Information Security Management Collection Chapter 2 – Understanding Information Value* § 13
E9.080	INM-040	The organisation applies appropriate protective markings to information throughout its lifecycle.	*VPDSF Information Security Management Collection Chapter 3 – Protective Markings* § 23
E9.090	INF-070	The organisation manages the aggregated value of official information.	*VPDSF Information Security Management Collection Chapter 2 – Understanding Information Value* § 13.4.4
E9.100	INF-080	The organisation continually reviews the value of official information across the information lifecycle.	*VPDSF Information Security Management Collection Chapter 2 – Understanding Information Value* § 19

E9.110		The organisation manages externally generated information in accordance with the originator's instructions.	*VPDSF Information Security Management Collection Chapter 3 – Protective Markings* § 24

Change log

Title

- Change numbering from Standard 13 and 14 to Standard 9
- Due to the merging of two standards, change 'Information Value' and 'Information Management' with an overarching title 'Security aspects of information management'

Standard

- Replace the wording to be specific that this standard covers identification and assessment of information and the application of controls to cover both information security centric standards
- Change to active voice (removes 'must' language)

Objective

- Replace 'public sector data' with 'official information'
- Add 'identification' phase
- Replace 'valuation criteria' with 'assessment criteria'
- Include the 'confidentiality, integrity and availability' because taken out of the standard
- Retain the 'lifecycle' concept from the Information Management standard

Controls

- Remove reference to Public Record Office of Victoria (PROV) Standards and Policies
- Remove reference to DataVic Access Policy
- Remove reference to PSPF

Elements

- Reorder for logical flow
- INF-030 Provide further explanation of security attributes 'confidentiality, integrity and availability business impact levels'
- INF-050 Replace 'accountable roles' with 'roles and responsibilities' and add examples 'originator, owner, custodian'
- INF-070 Replace 'identified' with 'manage'
- INF-080 Add 'information lifecycle' to be clear that this relates to managing information from cradle to grave
- INM-010 Replace 'protective data security' with 'information security'
- Remove INM-020 (covered in INM-010)
- Remove INM-030 (covered by all the standards)
- Add new element E9.110 related to handling of externally generated information
- Change to active voice

Standard 10 – Personnel Security

Standard

An organisation establishes, implements and maintains personnel security controls addressing all persons continuing eligibility and suitability to access official information.

Statement of Objective

To mitigate an organisation's personnel security risks and provide a consistent approach for managing all persons with access to official information.

Elements

V2.0 #	V1.1 #	Element	Derivation
E10.010	PER-050	The organisation's personnel security policies and procedures addresses the personnel lifecycle phases of: * Pre-engagement * Engagement (ongoing and re-engagement) * Separating (permanently or temporarily)	*PSPF GOVSEC-2 Management structures and responsibilities* § C.6 *PSPF GOVSEC-3 Security planning and risk management* § C.2 Table 2 *PSPF PERSEC-13 Ongoing assessment of personnel* § C.1 Table 1
E10.020	PER-020	The organisation verifies the identity of personnel and re-validates it throughout the personnel lifecycle phases.	*PSPF PERSEC-12 Eligibility and suitability of personnel* § para 11 Table 1 Identity checks *National Identity Proofing Guidelines (NIPG)* § 4.1
E10.030	PER-030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-12 Eligibility and suitability of personnel*

			§ C1 Table 2
E10.040	PER-040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-13 Ongoing assessment of personnel* § C.1
E10.050		The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.	*PSPF PERSEC-14 Separating personnel*
Additional elements for organisations requiring security clearances			
E10.060	PER-060	The organisation develops security clearance policies and procedures to support roles requiring high assurance or handling security classified information.	*PSPF PERSEC-13 Ongoing assessment of personnel* § C.1 Table 1
E10.070	PER-070	The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance or handling security classified information.	*PSPF PERSEC-12 Eligibility and suitability of personnel* § C2 § C.2.1
E10.080	PER-080	The organisation actively monitors and manages security clearance holders.	*PSPF PERSEC-13 Ongoing assessment of personnel* § C.2

Change log

Title

- Change numbering from Standard 16 to Standard 10
- Replace 'Personnel Lifecycle' with 'Personnel Security'

Standard

- Replace 'in their personnel management regime' with 'addressing all persons continued eligibility and suitability to access official information' to expand what personnel security includes rather than dictate where it should sit within an organisation
- Change to active voice (removes 'must' language)

Objective

- Replace with wording regarding managing risks.
- Replace 'public sector data' with 'official information'
- Change to active voice

Controls

- Replace PSPF reference with GOVSEC-3 Security planning and risk management; PERSEC-12 Eligibility and suitability of personnel; PERSEC-13 Ongoing assessment of personnel; PERSEC-14 Separating personnel

Elements

- Remove PER-010 (covered by PER-050) i.e. policies and procedures regardless of where they reside in the organisation
- PER-050 Provide greater clarity on phases i.e. add ‘ongoing and re-engagement’ to engagement phase and replace ‘post-engagement’ with ‘separating’ to cover both permanent and temporary departures
- PER-020 Replace ‘engagement lifecycle’ with ‘personnel lifecycle phases’ for consistency
- PER-020 Replace ‘manage’ with ‘re-validate’
- PER-040, PER-030, PER-090 Add ‘commensurate with their security and probity obligations and risk profile’ for consistency and call out probity as a discrete consideration
- PER-060 and PER-070 Reorder to have ‘requiring high assurance’ first
- E10.050 Add new element related to managing personnel separating from the organisation to cover all phases of personnel security
- Change to active voice

Standard 11 – Information Communications Technology (ICT) Security

Standard

An organisation establishes, implements and maintains Information Communications Technology (ICT) security controls.

Statement of Objective

To maintain a secure environment by protecting the organisation's official information through ICT security controls.

Elements

V2.0 #	V1.1 #	Element	Derivation
E11.010	ICT-010	The organisation has security documentation for ICT systems e.g. system security plan.	*Australian Government Information Security Manual (ISM)* § Guidelines for security documentation
E11.020	ICT-020	The organisation manages all ICT assets throughout their lifecycle.	*ISM* § Guidelines for physical security § Guidelines for ICT equipment management
E11.030	ICT-040	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing or storing official information.	*ISM* § Guidelines for authorising systems
E11.040	ICT-050	The organisation manages vulnerabilities to its ICT systems throughout the ICT system lifecycle.	*ISM* § Guidelines for system monitoring
E11.050	ICT-060	The organisation documents and manages changes to ICT systems.	*ISM* § Guidelines for system management – Change management
E11.060	ICT-070	The organisation has communications security (cable management) controls.	*ISM* § Guidelines for communications infrastructure

E11.070	ICT-080	The organisation verifies the vendors security claims before implementing security technologies.	*ISM* § Guidelines for evaluated products
E11.080	ICT-090	The organisation has security measures (classification, labelling, usage, sanitisation, destruction, disposal) in place for media.	*ISM* § Guidelines for media management
E11.090	ICT-100	The organisation has hardened standard operating environments (SOEs) for workstations and servers commensurate with security risk.	*ISM* § Guidelines for system hardening
E11.100	ICT-110	The organisation has security measures for email use.	*ISM* § Guidelines for email management
E11.110	ICT-120	The organisation has system logging and monitoring to record events.	*ISM* § Guidelines for system monitoring
E11.120	ICT-130	The organisation has secure administration practices.	*ISM* § Guidelines for system management § Guidelines for personnel security - Privileged access to systems
E11.130	ICT-140	The organisation designs and configures the ICT network in a secure manner.	*ISM* § Guidelines for network management
E11.140	ICT-150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation and authentication commensurate with the risk to information.	*ISM* § Guidelines for using cryptography
E11.150	ICT-160	The organisation has a cryptographic policy governing key management.	*AS ISO/IEC 27002:2015* § 10.1.2
E11.160	ICT-170	The organisation has malware prevention and detection software installed on all ICT systems.	*ISM* § Guidelines for gateway management

			§ Guidelines for data transfers and content filtering
E11.170	ICT-190	The organisation has separate development, testing and production environments.	*ISM* § Guidelines for software development
E11.180	ICT-200	The organisation has a backup management system.	*ISM* § Guidelines for system management
E11.190	ICT-210	The organisation has a secure development lifecycle.	*ISM* § Guidelines for software development
E11.200		The organisation has security measures for enterprise mobility.	*ISM* § Guidelines for enterprise mobility

Change log

Title
- Change numbering from Standard 17 to Standard 11

Standard
- Remove reference to 'ICT Management regime' because do not believe it is necessary to dictate where it should sit within an organisation
- Change to active voice (removes 'must' language)

Objective
- Replace 'public sector data' with 'official information'
- Change to active voice

Controls
- Add reference to AS ISO/IEC 27002:2015 Code of practice for information security controls

Elements
- ICT-010 Provide an example of security documentation 'system security plan'
- ICT-040 – changed to align with ISM regarding authorising systems rather than formal accreditation framework
- Move ICT-030 related to disaster recovery plans to Standard 6 – Information Security aspects of Business Continuity
- ICT-070 Provide an example of communications security 'cable management'
- Remove ICT-180 (part of normal IT operations rather than specific to security)
- Add E11.200 regarding enterprise mobility to support a mobile workforce
- Change to active voice

Standard 12 – Physical Security

Standard

An organisation establishes, implements and maintains physical security controls addressing facilities, equipment and services.

Statement of Objective

To maintain a secure environment to protect the organisation's official information by applying physical security measures.

Elements

V2.0 #	V1.1 #	Element	Derivation
E12.010	PHY-010	The organisation plans and documents physical security measures.	*PSPF PHYSEC-16* § C1 § C2
E12.020	PHY-020	The organisation applies defence-in-depth physical security measures.	*Victorian Government Office Accommodation guidelines* § 2.6 § 4.7 *PSPF PHYSEC-16* § C2 § C4 *AS ISO/IEC 27002:2015* § 11.1
E12.030	PHY-050	The organisation selects physical security measures commensurate with the business impact level of the information.	*Victorian Government Office Accommodation guidelines* § 4.7 *PSPF PHYSEC-15* § C.2 § C.3 *PSPF PHYSEC-16* § C1 § C2 § C3 *AS ISO/IEC 27002:2015* § 11.2

E12.040	PHY-060	The organisation has scalable physical security measures ready for activation during increased threat situations.	*PSPF GOVSEC-3* § C3
E12.050	PHY-070	The organisation manages physical security measures when handling information out of the office.	*PSPF PHYSEC-15* § C.8 *AS ISO/IEC 27002:2015* § 11.2.6
E12.060	PHY-080	The organisation manages physical security measures throughout their lifecycle.	*PSPF PHYSEC-15* § C.7 *AS ISO/IEC 27002:2015* § 11.2.4 § 11.2.7

Change log

Title
- Change numbering from Standard 18 to Standard 12
- Replace 'Lifecycle' with 'Security'

Standard
- Replace 'in their physical management regime' with 'addressing facilities, equipment and services'
- Change to active voice (removes 'must' language)

Objective
- Replace 'public sector data' with 'official information'
- Remove 'facilities, equipment and services' because moved up to Standard statement
- Change to active voice

Controls
- Replace PSPF reference with PHYSEC-15 Physical security for entity resources and PHYSEC-16 Entity Facilities
- Add reference to AS ISO/IEC 27002:2015 Code of practice for information security controls

Elements
- Add 'physical security measures' throughout for consistency to cover 'facilities, equipment and services'
- PHY-010 Replace 'facilities and building management policies and procedures include' with 'plan and document' to be generic. Policies captured under *Standard 1 SMF*
- PHY-020 and PHY-040 Merge because cover similar concept i.e. defence-in-depth and zones (applying multiple controls in case one fails)
- PHY-020 Remove reference to 'protection of information' as all elements relate to protecting information
- PHY-030 and PHY-050 Merge because cover similar concept i.e. selection of physical security measures
- PHY-090 Remove because covered by 080 lifecycle
- Change to active voice